UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/937,396	12/06/2001	Jean-Sebastien Coron	032326-169	9410

21839 7590 04/19/2006

BUCHANAN INGERSOLL PC
(INCLUDING BURNS, DOANE, SWECKER & MATHIS)
POST OFFICE BOX 1404
ALEXANDRIA, VA 22313-1404

EXAMINER	
PATEL, NIRAV B	

ART UNIT	PAPER NUMBER
2135	

DATE MAILED: 04/19/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/937,396	CORON, JEAN-SEBASTIEN	
	Examiner	Art Unit	
	Nirav Patel	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *03 April 2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-13* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-13* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Applicant's amendment filed on April 3, 2006 has been fully considered and arguments are found persuasive. However, upon reconsidering claims 1-13, examiner has found the non-statutory subject matter in the pending claims 1-13.

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

2. Claims 1-13 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

Claim 1 recites "a countermeasure method in an electronic component implementing an an elliptical curve type public key encryption algorithm, wherein a point P on the elliptical curve is represented by projective coordinates (X, Y, Z) such that x = X/Z and y = Z^3, x and Y being the coordinates of the point on the elliptical curve in terms of affine coordinates said curve comprising n elements and being defined on a finite field GF (p), where p is a prime number and the curve has the equation y^2 = x^3 + a*x + b, or defined on a finite field GF (2^n), with the curve having the equation y^2 + x*y = x^3 + a*x^2 +b, where a and b are integer parameters, the method comprising the step of : drawing at random an integer λ such that $0 < \lambda < p$; For a point P represented by projective coordinates (X1, Y1, Z1), calculating X'1 = λ^2*X1, Y'1 = λ^3*Y1 and Z'1 = λ*Z1, to define the coordinates of the point P' = (X'1, Y'1, Z'1); calculating an output

point Q = 2*P' that is represented by projective coordinates (X2, Y2, Z2)". **Claim 1 is rejected under 35 USC 101 for failing to provide a practical application that produces a useful, tangible and concrete result. As per claim 1, the abstract idea is expressed as drawing at random integer, calculating the projective coordinates and calculating an output point using the calculated result. Therefor, Claim 1 consists solely of mathematical operation without some claimed practical application i.e. executing a mathematical algorithm, there is no tangible result provided to satisfy the practical application requirement of 35 USC 101. Therefor, claim 1 recites non-statutory subject matter.**

Claims 2-13 depend on claim 1, therefore they are rejected with the same rationale applied against claim 1 above.

Allowable Subject Matter

3. Claims 1-13 would be allowable if rewritten or amended to overcome the rejection(s) under 35 U.S.C. 101, set forth in this Office action.

Response to Argument

4. Applicant's arguments filed April 3, 2006 have been fully considered, and arguments are persuasive on the basis that the elements of the triplet are not multiplied by λ^2, λ^3 and λ respectively.

Conclusion

5. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Nirav Patel whose telephone number is 571-272-5936.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 571-272-3859. The fax and phone numbers for the organization where this application or proceeding is assigned is 571-273-8300.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 571-272-2100.

NBP
4/14/06

HOSUK SONG
PRIMARY EXAMINER